System Strategies

Description

System complexity, today, is an aggregate of technology, scale, scope, operational, and organizational issues. The business usage, the technologies applied, and the changing operational environment raise software risks that are typically not addressed in current practice. This section discusses the effects of the changing operational environment on the development of secure systems. Vulnerability analysis has typically concentrated on errors in coding or in the interfaces among components; however, system interactions can also be a seedbed for vulnerabilities. One article in this content area includes discussions of the software assurance challenges inherent in networked systems development and proposes a structured approach to analyzing potential system stresses using scenarios.

Note: At a future date, this content area will be moved to a new section of Build Security In that will focus on system issues.

Overview Articles

Name	Version Creation Time	Abstract
Introduction to System Strategies	5/16/08 2:39:02 PM	Trustworthiness can no longer be predicted by building software systems from discrete, isolated pieces that address static requirements within planned cost and schedule. Each new or updated component joins an existing operational environment and must merge with that legacy to form an operational whole. Today's technology must support an operating environment that is driven by business goals and organizational needs instead of a predefined infrastructure that functions within established technology constraints. The operating environment can be geographically and managerially distributed and dynamically changing. Few businesses can stop to make changes and then restart. This introduction discusses the effects of the changing operational environment on the development of secure systems.

Most Recently Updated Articles [Ordered by Last Modified Date]

Name	Version Creation Time	Abstract
Scale: System Development Challenges	5/16/08 2:39:02 PM	The usage and characteristics of large systems or systems of systems can challenge many

		current development assumptions. Vulnerability analysis has typically concentrated on vulnerabilities induced by errors in coding or in the interfaces among components. System interactions can also be a seedbed for vulnerabilities, however. This article describes software assurance challenges inherent in networked systems development and proposes a structured approach to analyzing potential system stresses using scenarios.
Introduction to System Strategies	5/16/08 2:39:02 PM	Trustworthiness can no longer be predicted by building software systems from discrete, isolated pieces that address static requirements within planned cost and schedule. Each new or updated component joins an existing operational environment and must merge with that legacy to form an operational whole. Today's technology must support an operating environment that is driven by business goals and organizational needs instead of a predefined infrastructure that functions within established technology constraints. The operating environment can be geographically and managerially distributed and dynamically changing. Few businesses can stop to make changes and then restart. This introduction discusses the effects of the changing operational environment on the development of secure systems.
System Strategies References	5/16/08 2:39:01 PM	System Strategies bibliography.

All Articles [Ordered by Title]

- Considering Operational Security Risk During System Development[1] [5/22/07 9:07:13 AM]
  The operational security of software-intensive systems is closely linked to the practices and techniques used during system design and development. The authors examine OCTAVE, an operational security-risk methodology, and apply it to the security-related risks identifiable while developing software-intensive systems.

Name	Version Creation Time	Abstract

Introduction to System Strategies	5/16/08 2:39:02 PM	Trustworthiness can no longer be predicted by building software systems from discrete, isolated pieces that address static requirements within planned cost and schedule. Each new or updated component joins an existing operational environment and must merge with that legacy to form an operational whole. Today's technology must support an operating environment that is driven by business goals and organizational needs instead of a predefined infrastructure that functions within established technology constraints. The operating environment can be geographically and managerially distributed and dynamically changing. Few businesses can stop to make changes and then restart. This introduction discusses the effects of the changing operational environment on the development of secure systems.
Scale: System Development Challenges	5/16/08 2:39:02 PM	The usage and characteristics of large systems or systems of systems can challenge many current development assumptions. Vulnerability analysis has typically concentrated on vulnerabilities induced by errors in coding or in the interfaces among components. System interactions can also be a seedbed for vulnerabilities, however. This article describes software assurance challenges inherent in networked systems development and proposes a structured approach to analyzing potential system stresses using scenarios.
System Strategies References	5/16/08 2:39:01 PM	System Strategies bibliography.